

RECEIVED
CENTRAL FAX CENTER

AUG 21 2006

Serial No. 09/863,583
Page 13 of 17REMARKS

Claim 2 had previously been canceled. Applicants cancel claims 3, 7, and 18. Claims 1, 4-6, 8-17, and 19-28 remaining pending in the application. Applicants amend claims 1 and 4 to incorporate the features of canceled claim 3, and amend claims 5 and 6 to incorporate features of canceled claims 7 and 18, respectively. Applicants also amend claims 8, 17, 19, 23 and 27 for proper dependency. No new matter has been added.

The Examiner objected to claims 1 and 4-6 for a number of apparent informalities. Applicants amend claims 1 and 4-6 in accordance with the Examiner's suggestions, and respectfully request that the Examiner withdraw the objection.

Claims 1, 3-7, 10-14, 17-18, 21-25, 27-28 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,818,936 to Mashayekhi in view of U.S. Patent No. 5,761,309 to Ohashi et al., and further in view of U.S. Patent No. 6,981,147 to Hamann et al.; and claims 8-9, 15-16, 19-20, and 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Mashayekhi in view of Ohashi et al., further in view of Hamann et al., and further in view of U.S. Patent No. 5,892,828 to Perlman. Applicants amend claims 1 and 4-6 to incorporate features of claim 1, 7, and 18, respectively, in a good faith effort to further clarify the invention as distinguished from the cited references. Applicants respectfully traverse the rejections.

The Examiner cited new reference Hamann et al. as alleged disclosure of "grouping of certificates." The cited portions of Hamann et al. only describe, however, a group certificate in the context of a certificate that groups together "keys to be issued at the same time for the same

84156784_1.DOC

Serial No. 09/863,583

Page 14 of 17

user by the same certification instance.” Please see, e.g., the abstract of Hamann et al. As such, the “group certificate” for a user’s keys described in Hamann et al. does not disclose the claimed group certificate for a group to which a user belongs. Indeed, Hamann et al. only describe a certificate based on a public key, and an invention directed to simplifying the process and reducing the needed storage by sharing the same items among a plurality of certificates for the same user by the same certification instance when the plurality of certificates include the same items.

Thus, even assuming, that it would have been obvious to one skilled in the art to combine Mashyekhi, Ohashi et al., and Hamann et al., the combination would have, at most, suggested grouping together “keys to be issued at the same time for the same user by the same certification instance,” as described in Hamann et al. Such a combination would still have failed to disclose or suggest the claimed feature of a group certificate based on the information on the group to which the related user belongs and whose membership to which is thereby authenticated.

Furthermore, Hamann et al. only describe, in the “Background of the Invention,” the use of a hash before an encryption process as a possible way to reduce the amount of data. The combination of references, therefore, further fail to disclose or suggest the claimed feature of the cryptographic function being a hash function.

Mashayekhi also only describes public key encryption where an inquiry to an authentication service is performed every time authentication is requested (“on demand”) by an application program. And the described “keychain” is thereby supplied from the authentication service to the application program. Mashayekhi, thus, does not disclose or suggest the claimed indirect authentication with identical secret information for identical groups. Furthermore, the

84156784_1.DOC

Serial No. 09/863,583

Page 15 of 17

portion of Mashayekhi cited by the Examiner in rejecting the claimed feature of the cryptographic function being a hash function (col. 2, lines 5-8) only relates to one instance of extracting an encryption key using a hash function, the key is then used in a separate cryptographic function. Mashayekhi, therefore, fails to suggest the claimed feature of using a hash function as the cryptographic function.

Indeed, Hamann et al., Mashayekhi, and Ohashi et al. all fail to disclose or suggest the claimed feature of using a hash function as the cryptographic function.

As such, even assuming, arguendo, that it would have been obvious to one skilled in the art to combine Hamann et al., Mashayekhi, and Ohashi et al., the combination would still have failed to disclose or suggest,

“[a] system of distributed group management for indirectly authenticating membership of a user in a group in order to manage security for a client on a client side and a server for executing a remote processing request from the client side under a predetermined authorization assigned for every group, provided with

a group certificate issuing apparatus for issuing a group certificate on the client side based on original group information including the name of the group to which the related user belongs when there is said remote processing request and

a group certificate verification unit for verifying a legitimacy of said group certificate transmitted from the client side in said server, wherein

said group certificate issuing apparatus adds an issuance side processed value obtained by encrypting the information of the original group information by a cryptographic function to the original group information and defines this as the group certificate,

said group certificate verification unit processes part of the information included in the received group certificate by an identical cryptographic function to obtain a verification side processed value and performs said authentication by confirming that said issuance side processed value and said verification side processed value coincide,

84156784_1.DOC

Serial No. 09/863,583

Page 16 of 17

said group certificate issuing apparatus includes first secret information assigned to said groups in said original group information and performs the processing by said cryptographic function, said first secret information being held only by said group certificate issuing apparatus,

said group certificate verification unit includes second secret information assigned to the groups in part of information included in said received group certificate and performs the processing by said cryptographic function, said second secret information being held only by said group certificate verification unit,

said first secret information and said second secret information are identical secret information for identical groups, and

said cryptographic function is a hash function," as recited in claim 1. (Emphasis added)

Accordingly, Applicants respectfully submit that claim 1 is patentable over Mashayekhi, Ohashi et al., and Hamann et al., separately and in combination, for at least the above-stated reasons. Claims 4-6 incorporate features that correspond to those of claim 1 cited above, and are, therefore, together with claims 10-14, 17, 21-25, 27-28 dependent therefrom, respectively, patentable over the cited references for at least the same reasons.

The Examiner relied upon Perlman to specifically address the additional features recited in dependent claims 8-9, 15-16, 19-20, and 26. As such, the combination of this reference, even if obvious to one skilled in the art at the time the claimed invention was made, would still have failed to cure the above-described deficiencies of Mashayekhi, Ohashi et al., and Hamann et al. Accordingly, Applicants respectfully submit that claims 8-9, 15-16, 19-20, and 26 are patentable over the cited references for at least the above-stated reasons with regard to their respective base claims 5 and 6, from which they depend.

The above statements on the disclosure in the cited references represent the present opinions of the undersigned attorney. The Examiner is respectfully requested to specifically

84156784_1.DOC

Serial No. 09/863,583

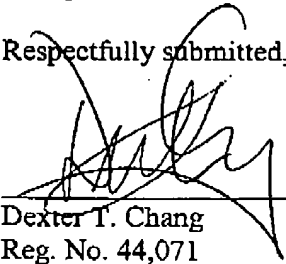
Page 17 of 17

indicate those portions of the respective reference that provide the basis for a view contrary to any of the above-stated opinions.

In view of the remarks set forth above, this application is in condition for allowance which action is respectfully requested. However, if for any reason the Examiner should consider this application not to be in condition for allowance, the Examiner is respectfully requested to telephone the undersigned attorney at the number listed below prior to issuing a further Action.

Any fee due with this paper may be charged to Deposit Account No. 50-1290.

Respectfully submitted,


Dexter T. Chang
Reg. No. 44,071

CUSTOMER NUMBER 026304
Telephone: (212) 940-6384
Fax: (212) 940-8986 or 8987
Docket No.: 100794-11702 (FUJA 18.671)
DTC:bf

84156784_1.DOC
NYC01_84156784_1_100794_11702